Algebra Univers. 72 (2014) 57–69
DOI 10.1007/s00012-014-0288-x
Published online May 23, 2014

Algebra Universalis

Uniform Mal'cev algebras with small congruence lattices

Nebojša Mudrinski

Abstract. A congruence of an algebra is called uniform if all the congruence classes are of the same size. An algebra is called uniform if each of its congruences is uniform. All algebras with a group reduct have this property. We prove that almost every finite uniform Mal'cev algebra with a congruence lattice of height at most two is polynomially equivalent to an expanded group.

1. Motivation

In this note, we investigate finite uniform algebras. We say that a congruence θ of an algebra $\mathbf{A}$ is *uniform* if all its congruence classes have the same cardinality. We say that an algebra $\mathbf{A}$ is uniform if all congruences of $\mathbf{A}$ are uniform. Uniform congruences have been introduced by W. Taylor in [13] and studied by R. McKenzie in [11]. In these papers, as in [4, p. 93], varieties of uniform algebras are considered rather than single uniform algebras. In 2005, K. Kaarli, [9], proved that finite uniform lattices are congruence permutable.

Clearly, all algebras with a group reduct (groups, rings and modules as the most famous examples) are uniform. Similarly, all quasigroups are also uniform and therefore all algebras with a quasigroup reduct (expanded quasigroups) are uniform. Let us recall that a *quasigroup* is a groupoid $(G, \cdot)$ such that for all $a, b \in G$ there exist unique x and y in G such that $ax = b$ and $ya = b$. Let a/θ and b/θ be two different classes of a congruence θ of the quasigroup G. We know that there is a $c \in G$ such that $a \cdot c = b$. We take the right translation $f_c\colon G \to G$, defined by $f_c(x) := x \cdot c$ for all $x \in G$, and restrict it to a/θ. Then $f_c(a/\theta) \subseteq b/\theta$ because θ is compatible with $\cdot$. Furthermore, f_c is an injective mapping because $\cdot$ is a quasigroup operation. Hence, $|a/\theta| \leq |b/\theta|$. Analogously, we obtain $|b/\theta| \leq |a/\theta|$. If $\cdot$ has a neutral element in G, then we call $(G, \cdot)$ a *loop*. An algebra $\mathbf{A}$ is called an *expanded quasigroup (loop)* if it has a quasigroup (loop) operation among its fundamental operations.

Presented by E. Kiss.
Received September 11, 2012; accepted in final form September 18, 2013.
2000 *Mathematics Subject Classification*: Primary: 08A30; Secondary: 20N05.
Key words and phrases: Mal'cev algebra, expanded group, expanded loop, uniform congruence.
Supported by the Austrian research fund FWF (P24077) and the Research Grant 174018 of the Ministry of Science and Education of the Republic of Serbia.

We say that two algebras on the same domain are *polynomially equivalent* if they have the same set of polynomials. One can show that every finite expanded quasigroup is polynomially equivalent to an expanded loop, see Proposition 2.1.

We restrict our investigation to the class of Mal'cev algebras. An algebra $\mathbf{A}$ is called a *Mal'cev algebra* if it has a *Mal'cev term*. This is a term function $d\colon A^3 \to A$ such that $d(x,y,y) = d(y,y,x) = x$ for all $x, y \in A$. In this note, by d we shall always denote a Mal'cev term. All previously mentioned classes of algebras: groups, rings, modules, expanded groups, quasigroups, loops, expanded quasigroups, and expanded loops are Mal'cev algebras. All these structures can be seen as expanded quasigroups (loops). Our goal is to characterize all finite uniform Mal'cev algebras. The question is:

Is there any finite Mal'cev algebra that is uniform and not polynomially equivalent to an expanded quasigroup (loop)?

The main result of this note is a partial answer to this question, given in Theorem 4.3. Namely, we prove that each finite uniform Mal'cev algebra with congruence lattice of height at most two is polynomially equivalent to an expanded loop. In many cases, these algebras will be polynomially equivalent to an expanded group.

2. Preliminaries

Proposition 2.1. *Every finite expanded quasigroup is polynomially equivalent to an expanded loop.*

Proof. Let f be a binary quasigroup operation of an expanded quasigroup $\mathbf{Q}$ and let $a \in Q$. We define a polynomial operation φ on Q such that $\varphi(x) := f(x,a)$ for all $x \in Q$. Let $|Q| = n$ for $n \in \mathbb{N}$. Then $\varphi^{n!} = id_Q$ because φ is a permutation on an n-element set. Now we define $g\colon Q^2 \to Q$ by $g(x,y) := f(\varphi^{(n!-1)}(x), y)$ for all $x, y \in Q$. Then we have $g(x,a) = \varphi^{n!}(x) = x$. If we define ψ on Q by $\psi(y) := g(a,y)$, then ψ is a permutation of Q, and therefore $\psi^{n!} = id_Q$. Finally, we define $h\colon Q^2 \to Q$ by $h(x,y) := g(x, \psi^{(n!-1)}(y))$ for all $x, y \in Q$. Then $h(a,y) = \psi^{n!}(y) = y$ for all $y \in Q$. Moreover, $h(x,a) = g(x,a)$ for all $x \in Q$ because $\psi(a) = a$. Hence, $h(x,a) = x$ for all $x \in Q$. One can easily observe that h is a binary polynomial quasigroup operation on Q. The neutral element with respect to h is a. □

The commutator $[\bullet, \bullet]$ is a binary operation on the congruence lattice of an algebra $\mathbf{A}$ (see [6, 12] for the explicit definition). If $\mathbf{A}$ is a Mal'cev algebra, then for all $\alpha, \beta, \gamma, \delta \in \mathsf{Con}\,\mathbf{A}$, $[\bullet, \bullet]$ satisfies the following properties:

(1) $[\alpha, \beta] \leq \alpha \wedge \beta$;
(2) if $\alpha \leq \gamma$ and $\beta \leq \delta$, then $[\alpha, \beta] \leq [\gamma, \delta]$;
(3) $[\alpha, \beta] = [\beta, \alpha]$;
(4) $[\alpha \vee \beta, \gamma] = [\alpha, \gamma] \vee [\beta, \gamma]$.

The first two properties are direct consequences of the definition of the commutator. For the proof of the last two of these properties, see [2, Lemma 2.5]. In this note, we shall use these properties without explicit reference. We shall call a congruence α of $\mathbf{A}$ *abelian* if $[\alpha, \alpha] = 0$. An algebra is *nilpotent* if the lower central series

$$[1, 1],\ [[1, 1], 1],\ \ldots,\ [\cdots[[1, 1], 1], \ldots, 1],\ \ldots$$

collapses to zero, see [6, p. 47]. Notice that every abelian algebra is nilpotent. An algebra $\mathbf{A}$ is *TC-neutral* if $[\alpha, \beta] = \alpha \wedge \beta$ for all $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$. One can prove using the commutator properties that the last condition is equivalent to $[\gamma, \gamma] = \gamma$ for all $\gamma \in \mathsf{Con}\,\mathbf{A}$. In a Mal'cev algebra $\mathbf{A}$, we call the largest congruence γ with the property $[\beta, \gamma] \leq \alpha$ the *centralizer of* β *modulo* α and denote it by $(\alpha : \beta)_{\mathbf{A}}$, [12, p. 252]. In [8], the condition (SC1) has been isolated as an important condition for describing polynomials in a certain class of algebras. By definition, a finite algebra $\mathbf{A}$ in a congruence modular variety satisfies the condition (SC1) if in every subdirectly irreducible homomorphic image $\mathbf{B}$ of $\mathbf{A}$ with monolith $\mu \in \mathsf{Con}\,\mathbf{B}$, we have $(0 : \mu)_{\mathbf{B}} \leq \mu$.

In order to use the results of [8], we need the following concepts from Tame Congruence Theory, [7]. In a finite algebra $\mathbf{A}$ with $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$, $U_{\mathbf{A}}(\alpha, \beta) = \{f(A) \mid f \in \mathsf{Pol}_1\mathbf{A}$ such that $f(\beta) \not\subseteq \alpha\}$, $M_{\mathbf{A}}(\alpha, \beta)$ is the set of all minimal members of $U_{\mathbf{A}}(\alpha, \beta)$ with respect to set inclusion, and if α is a subcover of β, $\mathsf{typ}\langle\alpha, \beta\rangle$ denotes the type of $\mathbf{A}|_U$ relative to $\langle\alpha|_U, \beta|_U\rangle$. Here,

$$\mathbf{A}|_U = (U, \{h \in \mathsf{Pol}_{\mathrm{n}}\mathbf{A} \mid n \in \mathbb{N}, h(U^n) \subseteq U\}).$$

For details, we refer to [7].

The *extended labelling* of the prime quotient $\langle\alpha, \beta\rangle$, according to [7, 8], is

(a) 3 if $[\beta, \beta] = \beta$;
(b) $(2, k)$ if $[\beta, \beta] = \alpha$.

In case (b), for each $U \in M_{\mathbf{A}}(\alpha, \beta)$, $\mathbf{A}|_U$ is polynomially equivalent to a vector space by [7, 8]. We define k to be the cardinality of the scalar field of this vector space.

In [8], the following new concept of polynomial completeness was introduced. We call an algebra $\mathbf{A}$ *weakly polynomially rich* if all the functions on A that preserve the congruence lattice and extended labellings of $\mathbf{A}$ are polynomial functions of $\mathbf{A}$.

The following special class of binary polynomials can be used to define commutators in Mal'cev algebras, as it has been done in [3, Lemma 6.9].

Definition 2.2. Let $\mathbf{A}$ be an algebra. We call a binary polynomial f of $\mathbf{A}$ *absorbing at* $(a, b) \in A^2$ if $f(a, y) = f(x, b) = f(a, b)$ for all $x, y \in A$.

Now we give a specialization of [3, Lemma 6.9] for binary commutators.

Lemma 2.3 (cf. [3, Lemma 6.9]). *Let* $\mathbf{A}$ *be a Mal'cev algebra and let* $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$. *Then* $[\alpha, \beta]$ *is generated as a congruence by the set*

$$R = \big\{(c(b_1, b_2), c(a_1, a_2)) \mid b_1, b_2, a_1, a_2 \in A,\ a_1 \equiv b_1 \pmod{\alpha},\ a_2 \equiv b_2 \pmod{\beta},\ c \in \mathsf{Pol}_2\mathbf{A} \text{ is absorbing at } (a_1, a_2)\big\}.$$

We denote the smallest congruence of an algebra $\mathbf{A}$ that contains $(x, y) \in A^2$ by $\Theta_{\mathbf{A}}(x, y)$. Such a congruence we call a *principal congruence*. If α and β are principal congruences of a Mal'cev algebra $\mathbf{A}$, then the previous lemma can be simplified.

Lemma 2.4 (cf. [3, Lemma 6.13]). *Let* $\mathbf{A}$ *be a Mal'cev algebra and let* $\alpha, \beta \in \mathsf{Con}\,\mathbf{A}$ *be such that* $\alpha = \Theta_{\mathbf{A}}(u_1, v_1)$ *and* $\beta = \Theta_{\mathbf{A}}(u_2, v_2)$ *for some* u_1, u_2, v_1, v_2 *in* A. *Then*

$$[\alpha, \beta] = \{(c(v_1, v_2), c(u_1, u_2)) \mid c \in \mathsf{Pol}_2\mathbf{A} \text{ is absorbing at } (u_1, u_2)\}.$$

As usual, for each congruence θ of an algebra $\mathbf{A}$ and each congruence preserving n-ary function f on A for $n \in \mathbb{N}$, we define an n-ary function f/θ on A/θ by $f/\theta(x_1/\theta, \dots, x_n/\theta) := f(x_1, \dots, x_n)/\theta$ for all $x_1/\theta, \dots, x_n/\theta \in A/\theta$.

By $\mathbf{A} + f$, we denote the algebra obtained from an algebra $\mathbf{A}$ by adding a new fundamental operation f on A.

Definition 2.5. Let θ be a proper non-trivial uniform equivalence relation on a set A such that $|A/\theta| = m + 1$ and $|a/\theta| = n + 1$, for all $a \in A$. If we denote the elements of A by a_{ij}, such that

$$a_{ij} \equiv_\theta a_{kl} \iff i = k, \tag{2.1}$$

for all $i, k \in \{0, \dots, m\}$ and $j, l \in \{0, \dots, n\}$, we call such an enumeration a *θ-enumeration*.

Furthermore, if

$$\oplus\colon \{0, \dots, m\}^2 \to \{0, \dots, m\} \text{ and } +\colon \{0, \dots, n\}^2 \to \{0, \dots, n\},$$

then we define $f_{\oplus,+}\colon A^2 \to A$ by

$$f_{\oplus,+}(a_{ij}, a_{kl}) := a_{i\oplus k, j+l}, \tag{2.2}$$

and call it an *index defined operation* $f_{\oplus,+}$.

Let us observe that an index defined operation $f_{\oplus,+}$ preserves θ for each θ-enumeration a_{ij} and all binary operations $\oplus$ on $\{0, \dots, m\}$ and $+$ on $\{0, \dots, n\}$.

If a θ-enumeration a_{ij} has been made, then we shall always denote by I the mapping that gives back the first index of the element that represents an equivalence class of the equivalence relation θ. More precisely, we define the function $I\colon A/\theta \to \{0, \dots, m\}$ such that $I(a_{ij}/\theta) := i$, where $|A/\theta| = m + 1$. It is not hard to check that I is a well-defined bijection.

Definition 2.6. Let $\mathbf{A}$ be a finite set with a uniform equivalence relation $\theta, 0 < \theta < 1$, and let a_{ij} be a θ-enumeration of the elements of A such that

$|A/\theta| = m+1$ and $|a/\theta| = n+1$ for all $a \in A$. If $+$ is a binary operation on A/θ then a binary operation $\oplus\colon \{0,\dots,m\}^2 \to \{0,\dots,m\}$ defined by $i \oplus j := I(a_{i0}/\theta + a_{j0}/\theta)$, we call a $(\theta,+)$ *corresponding first index operation.*

Corollary 2.7. *Let A be a finite set with a uniform equivalence relation θ with $0 < \theta < 1$, and let a_{ij} be a θ-enumeration of the elements of A such that $|A/\theta| = m+1$ and $|a/\theta| = n+1$ for all $a \in A$. If $+$ is a binary operation on A/θ and $\oplus$ is the $(\theta,+)$ corresponding first index operation, then I is an isomorphism from $(A/\theta,+)$ to $(\{0,\dots,m\},\oplus)$.*

Proof. This follows directly from the definition of I and Definition 2.6. □

An algebra is *affine complete* if all congruence preserving functions on the domain are polynomials. We call an algebra *functionally complete* if all functions on the domain are polynomials. The statements in the following proposition are well known facts, but are also a consequence of [1, Proposition 5.2].

Proposition 2.8. *Every finite TC-neutral Mal'cev algebra is affine complete. Especially, every finite simple non-abelian Mal'cev algebra is functionally complete.*

3. Expanded groups

In this section, we prove that every finite uniform Mal'cev algebra with congruence lattice of height at most two is polynomially equivalent to an expanded group except if the algebra is 2-nilpotent and its congruence lattice is the three element chain.

Proposition 3.1. *If $\mathbf{A}$ is a Mal'cev algebra with congruence lattice isomorphic to $\mathbf{M}_i$ for $i \geq 3$, then $\mathbf{A}$ is polynomially equivalent to an expanded group.*

Proof. It is well known that in this case, $\mathbf{A}$ is abelian and therefore polynomially equivalent to a module over a ring. □

Proposition 3.2. *If $\mathbf{A}$ be a finite simple Mal'cev algebra, then $\mathbf{A}$ is polynomially equivalent to an expanded group.*

Proof. If $[1,1] = 0$, then $\mathbf{A}$ is polynomially equivalent to a module over a ring and so the statement is true. If $[1,1] = 1$, then $\mathbf{A}$ is TC-neutral. We define any group operation on $\mathbf{A}$. It is a polynomial of $\mathbf{A}$ by Proposition 2.8. □

We say that an algebra $\mathbf{A}$ has no *skew congruences* between congruences α and β of $\mathbf{A}$ if $\gamma = (\gamma \wedge \alpha) \vee (\gamma \wedge \beta)$ for all $\gamma \in \mathsf{Con}\,\mathbf{A}$ such that $\alpha \wedge \beta \leq \gamma \leq \alpha \vee \beta$.

Proposition 3.3. *Let $\mathbf{A}$ be a finite Mal'cev algebra with congruence lattice isomorphic to $\mathbf{M}_2$. Then $\mathbf{A}$ is polynomially equivalent to an expanded group.*

Proof. Let $\theta, \varphi \in \mathsf{Con}\,\mathbf{A} \backslash \{0,1\}$. Then $\mathbf{A}/\theta$ and $\mathbf{A}/\varphi$ are simple algebras and $\mathbf{A} \cong \mathbf{A}/\theta \times \mathbf{A}/\varphi$. By Proposition 3.2, we know that there exist polynomials

d_1 and d_2 such that d_1/θ is a polynomial group operation of $\mathbf{A}/\theta$ and d_2/φ is a polynomial group operation of $\mathbf{A}/\varphi$. We define a binary operation f on $A/\theta \times A/\varphi$ for all $(x_1/\theta, y_1/\varphi), (x_2/\theta, y_2/\varphi) \in A/\theta \times A/\varphi$ by

$$f((x_1/\theta, y_1/\varphi), (x_2/\theta, y_2/\varphi)) := (d_1(x_1, x_2)/\theta, d_2(y_1, y_2)/\varphi).$$

Clearly, f is a group operation that preserves θ and φ such that $f/\theta = d_1/\theta$ and $f/\varphi = d_2/\varphi$. There are no skew congruences between θ and φ. Hence, f is a polynomial of $\mathbf{A}$, by [10, Theorem 1]. Therefore, we obtain that $\mathbf{A}$ is polynomially equivalent to an expanded group. □

Now the only other possibility for the congruence lattice of a finite uniform Mal'cev algebra if it is of height at most two is the three element chain. This case involves a bit more of work. We are going to show that the index defined operation is the desired polynomial group operation. Depending on the behavior of the commutator operation, we choose operations on indexes in appropriate way.

Proposition 3.4. *Let A be a set with a uniform equivalence relation θ. Then for every group operation $+$ on A/θ, there exists a group operation on A that preserves θ and induces $+$ modulo θ.*

Proof. Let $m, n \in \mathbb{N}$ be such that $|A/\theta| = m + 1$ and $|a/\theta| = n + 1$ for all $a \in A$, and let a_{ij} be a θ-enumeration of the elements of A. Then for $(\theta, +)$ corresponding first index operation $\oplus$ on $\{0, \dots, m\}$ and each group operation $\cdot$ on $\{0, \dots, n\}$, the index defined operation $f_{\oplus,\cdot} \colon A^2 \to A$ is a group operation that preserves θ, because $\oplus$ is a group operation on $\{0, \dots, m\}$ by Corollary 2.7. Obviously, $f_{\oplus,\cdot}$ induces $+$ modulo θ. □

Proposition 3.5. *Let $\mathbf{A}$ be a finite uniform Mal'cev algebra with congruence lattice $\{0, \theta, 1\}$, where θ is non-abelian. Then $\mathbf{A}$ is polynomially equivalent to an expanded group.*

Proof. By Proposition 3.2, there exists a polynomial group operation $+$ on A/θ. By Proposition 3.4, there exists a group operation f on A that is compatible with θ and induces $+$ modulo θ. Hence, by [10, Corollary 14], f is a polynomial of $\mathbf{A}$. □

Let θ be a uniform congruence of a finite Mal'cev algebra $\mathbf{A}$. If a_{ij} is a θ-enumeration of the elements of A, then for the sequel, we define the binary operation $+_i$ on a_{i0}/θ by $a_{ik} +_i a_{il} := d(a_{ik}, a_{i0}, a_{il})$, for all $a_{ik}, a_{il} \in a_{i0}/\theta$ and for all $i \in \{0, \dots, m\}$. If $[\theta, \theta] = 0$, then $+_i$ is a commutative group operation on a_{i0}/θ, by [12, p. 256].

To choose an appropriate operation on the second index in a θ-enumeration, we need the following refinement of θ-enumeration. We are going to use it in Proposition 3.12, after we prove Lemma 3.9, 3.10, and 3.11 as important tools.

Definition 3.6. Let θ be a proper nontrivial uniform abelian congruence of an algebra $\mathbf{A}$ such that $|A/\theta| = m+1$ and $|a/\theta| = n+1$ for all $a \in A$. Then we

call a θ-enumeration a_{ij} of the elements of A a *suitable θ-enumeration* if for all $i, j \in \{0, \ldots, m\}$, the function $q_{ij} \colon a_{i0}/\theta \to a_{j0}/\theta$ defined by $q_{ij}(a_{ik}) := a_{jk}$, for all $k \in \{0, \ldots, n\}$, is a polynomial isomorphism between groups $(a_{i0}/\theta, +_i)$ and $(a_{j0}/\theta, +_j)$.

Lemma 3.7. *A finite uniform Mal'cev algebra with minimal abelian congruence θ admits a suitable θ-enumeration.*

Proof. Let $m, n \in \mathbb{N}$ be such that $|A/\theta| = m + 1$ and $|a/\theta| = n + 1$ for all $a \in A$. If $\{a_{00}, \ldots, a_{m0}\}$ is a transversal of θ, we shall show that all other elements of A can be denoted by a_{ij}, for $i \in \{0, \ldots, m\}$ and $j \in \{1, \ldots, n\}$, such that a_{ij} is a suitable θ-enumeration.

We define $R_{ij} := \{p \in \mathsf{Pol}_1\mathbf{A} \mid p(a_{j0}) = a_{i0}\}$ for all $i, j \in \{0, \ldots, m\}$. Let R be the set of all matrices $[r_{ij}]_{(m+1)\times(m+1)}$, where $r_{ij} \in R_{ij}$ for all $i, j \in \{0, \ldots, m\}$. Then $\mathbf{R}$ is a ring. If $\mathbf{M}$ is the direct product of the groups $(a_{00}/\theta, +_0), \ldots, (a_{m0}/\theta, +_m)$, then $\mathbf{M}$ is a simple module over the ring $\mathbf{R}$, and therefore $\mathbf{R}$ is a primitive ring, see [5, p. 150]. We know that the endomorphism ring $\mathbf{D}$ of $\mathbf{M}$ is a division ring by Schur's lemma. Moreover, $(a_{i0}/\theta, +_i)$ is a vector space over $\mathbf{D}$, R_{ii} is exactly the set of all $\mathbf{D}$-linear transformations of $(a_{i0}/\theta, +_i)$, and R_{ji} is exactly the set of all $\mathbf{D}$-linear transformations that map $(a_{i0}/\theta, +_i)$ into $(a_{j0}/\theta, +_j)$, for all $i, j \in \{0, \ldots, m\}$, by [5, p. 151]. Since all θ-classes are of the same finite cardinality, they are isomorphic as vector spaces. Each vector space isomorphism from $(a_{i0}/\theta, +_i)$ to $(a_{j0}/\theta, +_j)$ is a linear transformation and therefore a polynomial from R_{ji}, for all $i, j \in \{0, \ldots, m\}$.

We denote the elements of a_{00}/θ by $a_{00}, \ldots, a_{0n}$. For all $i \in \{0, \ldots, m-1\}$, we let $p_i \in R_{i+1,i}$ be an isomorphism from $(a_{i0}/\theta, +_i)$ to $(a_{i+1,0}/\theta, +_{i+1})$. Then we define $a_{i+1,j} := p_i(a_{ij})$ for all $j \in \{1, \ldots, n\}$. Clearly, this is a θ-enumeration. We define $p_m \colon a_{m0}/\theta \to a_{00}/\theta$ by $p_m(a_{mj}) := a_{0j}$ for all $j \in \{0, \ldots, n\}$. Obviously, $p_m \circ p_{m-1} \circ \cdots \circ p_0$ is the identity mapping on a_{00}/θ and $p_{m-1} \circ \cdots \circ p_0 \circ p_m$ is the identity mapping on a_{m0}/θ. Therefore, p_m is the inverse function of the isomorphism $p_{m-1} \circ \cdots \circ p_0$ from $(a_{00}/\theta, +_0)$ to $(a_{m0}/\theta, +_m)$. Hence, p_m is an isomorphism and linear transformation from $(a_{m0}/\theta, +_m)$ to $(a_{00}/\theta, +_0)$. Then we know that $p_m \in R_{0m}$. Now, for a given $i, j \in \{0, \ldots, m\}$, we define the polynomial isomorphism $q_{ij} \colon a_{i0}/\theta \to a_{j0}/\theta$ by

$$q_{ij} := \begin{cases} id, & \text{if } i = j; \\ p_{j-1} \circ \cdots \circ p_i, & \text{if } i < j; \\ p_{j-1} \circ \cdots \circ p_0 \circ p_m \circ \cdots \circ p_i, & \text{if } i > j > 0; \\ p_m \circ \cdots \circ p_i, & \text{if } j = 0. \end{cases}$$

Therefore, a_{ij} is a suitable θ-enumeration. □

Proposition 3.8. *Let $\mathbf{A}$ be a finite Mal'cev algebra and let f be a congruence-preserving operation on A. If there is an $\langle\alpha, \beta\rangle$-minimal set U in $\mathbf{A}$ such that U is $\langle\alpha, \beta\rangle$-minimal in $\mathbf{A} + f$ and $\mathbf{A}|_U$ is polynomially equivalent to $(\mathbf{A} + f)|_U$,*

then f preserves the extended labelling of the prime quotient $\langle\alpha,\beta\rangle$ in the congruence lattice of $\mathbf{A}$.

Proof. Directly by the definition of the extended labelling. □

Lemma 3.9. *Let $\mathbf{A}$ be a finite uniform Mal'cev algebra with congruence lattice $\{0,\theta,1\}$ such that $[1,1]=[1,\theta]=\theta$. Then there exists a unary polynomial e such that $e(A)$ is contained in a single θ-class and $e(\theta)\neq 0_{\mathbf{A}}$.*

Proof. Since $\theta<1$ we have $|A/\theta|\geq 2$ and each θ class has at least two elements, because θ is uniform and $\theta\neq 0$. Let $a,b\in A$, $u\notin a/\theta$, and $v\in b/\theta$ with $v\neq b$. Then we have $\Theta_{\mathbf{A}}(a,u)=1$ and $\Theta_{\mathbf{A}}(b,v)=\theta$. Using the assumption $[1,\theta]=\theta\neq 0$, we obtain a binary absorbing polynomial at (a,b) denoted by c such that $c(u,v)\neq c(a,b)$, by Lemma 2.4. Then $e\in \mathsf{Pol}_1\mathbf{A}$, defined by $e(x):=c(u,x)$ for all $x\in A$, is nonconstant on b/θ, because

$$e(v)=c(u,v)\neq c(a,b)=c(u,b)=e(b).$$

We have $c(a,x)\equiv_{[1,1]} c(a,b)$ because $c(a,x)=c(a,b)$, and therefore we obtain $e(x)=c(u,x)\equiv_{[1,1]} c(u,b)=c(a,b)$ for all $x\in A$. Hence, the polynomial e satisfies the conditions of the lemma. □

Lemma 3.10. *Let $\mathbf{A}$ be a finite Mal'cev algebra with $\mathsf{Con}\,\mathbf{A}=\{0,\theta,1\}$ such that $[1,1]=1$, $[1,\theta]=\theta$, and $[\theta,\theta]=0$. Then for each $a\in A$, there exists a unary polynomial e such that $e(A)\subseteq a/\theta$ and $e|_{a/\theta}=id_{a/\theta}$.*

Proof. Let $a\in A$ and let M be a maximal subset of A such that $a/\theta\subseteq M$ and

$$(\exists e\in \mathsf{Pol}_1\mathbf{A})(e|_{a/\theta}=id|_{a/\theta}\wedge e(M)\subseteq a/\theta).$$

Let us suppose that $M\neq A$. Let $e\in\mathsf{Pol}_1\mathbf{A}$ be such that $e|_{a/\theta}=id|_{a/\theta}$ and $e(M)\subseteq a/\theta$. Then there exists a $u\in A$ such that $u\notin M$ and $e(u)\notin a/\theta$. We denote $e(u)$ by v. Now we have $u,v\notin a/\theta$. Hence, we obtain $\Theta_{\mathbf{A}}(u,a)=\Theta_{\mathbf{A}}(v,a)=1$. Therefore, for each $b\in v/\theta$, $(b,a)\in 1=[1,1]=[\Theta_{\mathbf{A}}(u,a),\Theta_{\mathbf{A}}(v,a)]$. Hence, there exists an absorbing polynomial c that is absorbing at (a,a), $b=c(u,v)$, and $a=c(a,a)$, by Lemma 2.4. We know that $(u,a)\in 1=\Theta_{\mathbf{A}}(v,a)$. Hence, we have $p\in\mathsf{Pol}_1\mathbf{A}$ such that $p(v)=u$ and $p(a)=a$. Now we define the polynomial q by $q(x):=c(p(x),x)$ for all $x\in A$. Then

$$q(v)=c(p(v),v)=c(u,v)=b\equiv_\theta v. \tag{3.1}$$

Furthermore, for all $w\in a/\theta$, we have $p(w)\in a/\theta$. Hence, $c(p(w),w)\equiv_{[\theta,\theta]} c(a,a)=a$ by Lemma 2.3. Using the assumption $[\theta,\theta]=0$, we obtain $c(p(w),w)=a$. Therefore, $q(a/\theta)=\{a\}$. Now we define $e'\in\mathsf{Pol}_1\mathbf{A}$ by $e'(x):=d(e(x),q(e(x)),a)$ for all $x\in A$. One can see that $e'|_{a/\theta}=id|_{a/\theta}$, $e'(M)=e(M)\subseteq a/\theta$, and $e'(u)=d(e(u),q(e(u)),a)=d(v,q(v),a)\in a/\theta$, using (3.1). Therefore, the formula

$$(\exists e\in\mathsf{Pol}_1\mathbf{A})(e|_{a/\theta}=id|_{a/\theta}\wedge e(M\cup\{u\})\subseteq a/\theta)$$

is true. This is a contradiction with the maximality of M. □

Lemma 3.11. *Let* $\mathbf{A}$ *be a finite uniform nonabelian Mal'cev algebra with congruence lattice* $\{0, \theta, 1\}$. *If* θ *is abelian but not central, then there exists a* $\langle 0, \theta\rangle$*-minimal set* U *that is contained in a single* θ*-class.*

Proof. By the assumptions, we have $[1, \theta] = \theta$ and $[\theta, \theta] = 0$. If $[1, 1] = \theta$, then by Lemma 3.9, there is an $e \in \mathsf{Pol}_1\mathbf{A}$ such that $e(\theta) \neq 0_{\mathbf{A}}$ and $e(A)$ is contained in a single θ-class. If $[1, 1] = 1$, then by Lemma 3.10, there is an $e \in \mathsf{Pol}_1\mathbf{A}$ such that $e(\theta) \neq 0_{\mathbf{A}}$ and $e(A)$ is contained in the single θ-class. The statement of the Lemma follows now by the definition of minimal sets. □

Proposition 3.12. *Let* $\mathbf{A}$ *be a uniform Mal'cev algebra with a minimal abelian congruence* θ *such that* $|A/\theta| = m+1$ *and* $|a/\theta| = n+1$ *for all* $a \in A$. *Let* a_{ij} *be a suitable* θ*-enumeration of the elements of* A. *We define the operation* $+$ *on* $\{0, \dots, n\}$ *by*

$$j + k = l \text{ iff } a_{0j} +_0 a_{0k} = a_{0l}, \tag{3.2}$$

for all $j, k, l \in \{0, \dots, n\}$. *Then* $+$ *is a group operation on* $\{0, \dots, n\}$ *and* $a_{ij} +_i a_{ik} = a_{i,j+k}$ *for all* $i \in \{0, \dots, m\}$ *and* $j, k \in \{0, \dots, n\}$.

Proof. Obviously, $+$ is a group operation on $\{0, \dots, n\}$ because $+_0$ is a group operation. Since a_{ij} is a suitable θ-enumeration, there exists a polynomial isomorphism $q_{i0} \colon a_{i0}/\theta \to a_{00}/\theta$ between groups $(a_{i0}/\theta, +_i)$ and $(a_{00}/\theta, +_0)$ for all $i \in \{0, \dots, m\}$ such that $q_{i0}(a_{ij}) = a_{0j}$ for all $j \in \{0, \dots, n\}$, by Definition 3.6. The statement is true for $i = 0$ by (3.2). Let us fix $i \in \{1, \dots, m\}$. Now we obtain

$$a_{ij} +_i a_{ik} = q_{0i}(a_{0j}) +_i q_{0i}(a_{0k}) = q_{0i}(a_{0j} +_0 a_{0k}) = q_{0i}(a_{0,j+k}) = a_{i,j+k}. \quad \square$$

Lemma 3.13. *Let* $\mathbf{A}$ *be a finite uniform nonabelian Mal'cev algebra with congruence lattice* $\{0, \theta, 1\}$. *If* θ *is abelian but not central, then there exists a* θ*-enumeration* a_{ij} *of the elements of* A *and a group operation* $+$ *on the second index set such that for all group operations* $\oplus$ *on the first index set, the index defined operation* $f_{\oplus,+}$ *preserves the extended labelling of* $\langle 0, \theta\rangle$.

Proof. Let $m, n \in \mathbb{N}$ be such that $|A/\theta| = m + 1$ and $|a/\theta| = n + 1$ for all $a \in A$. According to Lemma 3.7, there is a suitable θ-enumeration a_{ij} of the elements of A. By Definition 3.6, there exist polynomial isomorphisms q_{ij} between groups $(a_{i0}/\theta, +_i)$ and $(a_{j0}/\theta, +_j)$ for all $i, j \in \{0, \dots, m\}$, defined by $q_{ij}(a_{ik}) = a_{jk}$ for all $k \in \{0, \dots, n\}$. Let $\oplus$ be any group operation on the set $\{0, \dots, m\}$ and let $+$ be a group operation on the set $\{0, \dots, n\}$ defined as in (3.2). We denote the index defined operation $f_{\oplus,+}$ shortly by f.

By Lemma 3.11, there exists a $\langle 0, \theta\rangle$-minimal set U of $\mathbf{A}$ such that $U \subseteq a/\theta$ for an $a \in A$. Then there exists a $g \in \mathsf{Pol}_1\mathbf{A}$ such that g is idempotent and $g(A) = U$. Let us suppose that U is not $\langle 0, \theta\rangle$-minimal in $\mathbf{A} + f$. Then there exists a $V \subsetneq U$ such that V is $\langle 0, \theta\rangle$-minimal in $\mathbf{A} + f$. Hence, we have $h \in \mathsf{Pol}_1(\mathbf{A} + f)$ such that $h(A) = V$ and h is idempotent. Now we obtain $V = h(V) \subseteq h(U) \subseteq h(A) = V$. Therefore, $h(U) = V$ and $(h \circ g)(A) = V$. We shall prove that there exists a polynomial h' of $\mathbf{A}$ such that $h'(U) = h(U)$ by

induction on the number of occurrences of f in the composition of fundamental operations, constants, and projections that represent h. First, we suppose that f occurs at least once in such a composition. Then there exist a $p \in \mathsf{Pol}_1\mathbf{A}$ and $p_1, p_2 \in \mathsf{Pol}_1(\mathbf{A}+f)$ such that $h = p(f(p_1,p_2))$. Now $(h \circ g)(A) = p(f(p_1,p_2))(g(A)) = p(f(p_1,p_2))(U)$. Next, we shall find $f' \in \mathsf{Pol}_2\mathbf{A}$ such that $f'(p_1,p_2)(U) = f(p_1,p_2)(U)$. We know that there exist $i,k \in \{0,\dots,m\}$ such that $p_1(U) \subseteq a_{i0}/\theta$ and $p_2(U) \subseteq a_{k0}/\theta$, because $U \subseteq a/\theta$, and that p_1 and p_2 preserve congruence θ because f preserves congruence θ. Now we define $f' \in \mathsf{Pol}_2\mathbf{A}$ by

$$f'(x,y) := d(q_{i,i\oplus k}(x), q_{0,i\oplus k}(a_{00}), q_{k,i\oplus k}(y)),$$

for all $x,y \in A$. Let $u \in U$ with $p_1(u) = a_{ij}$ and $p_2(u) = a_{kl}$. Then using Proposition 3.12, we have

$$\begin{aligned} f'(p_1(u),p_2(u)) &= f'(a_{ij},a_{kl}) = d(q_{i,i\oplus k}(a_{ij}), q_{0,i\oplus k}(a_{00}), q_{k,i\oplus k}(a_{kl})) \\ &= d(a_{i\oplus k,j}, a_{i\oplus k,0}, a_{i\oplus k,l}) = a_{i\oplus k,j} +_{i\oplus k} a_{i\oplus k,l} \\ &= a_{i\oplus k,j+l} = f(a_{ij},a_{kl}) = f(p_1(u),p_2(u)). \end{aligned}$$

Hence, we have proved that $f(p_1,p_2)(x) = f(p_1(x),p_2(x)) = f'(p_1(x),p_2(x)) = f'(p_1,p_2)(x)$, for all $x \in U$. Obviously, the number of occurrences of f in the composition of fundamental operations, constants, and projections that represent $p(f'(p_1,p_2))$ is smaller than the number of occurrences of f in the composition of fundamental operations, constants, and projections that represent $p(f(p_1,p_2))$. By the induction hypothesis, there exists an $h' \in \mathsf{Pol}_1\mathbf{A}$ such that $(h' \circ g)(A) = h'(U) = h(U) = V$. This contradicts the minimality of U because $h' \circ g \in \mathsf{Pol}_1\mathbf{A}$. Therefore, U is a $\langle 0,\theta\rangle$-minimal set of $\mathbf{A}+f$. In the same way, we prove that $\mathbf{A}|_U$ is polynomially equivalent to $(\mathbf{A}+f)|_U$. Using Proposition 3.8, we obtain that f preserves the extended labelling of $\langle 0,\theta\rangle$. □

Lemma 3.14. *Let $\mathbf{A}$ be a finite Mal'cev algebra with the unique nontrivial proper congruence θ. If an operation f on A is congruence preserving and $f/\theta \in \mathsf{Pol}(\mathbf{A}/\theta)$, then f preserves the extended labelling of the prime quotient $\langle\theta,1\rangle$.*

Proof. Since $f/\theta \in \mathsf{Pol}(\mathbf{A}/\theta)$, we obtain $\mathsf{Pol}((\mathbf{A}+f)/\theta) = \mathsf{Pol}(\mathbf{A}/\theta)$. Therefore, the extended labelling of $\langle 0,1\rangle$ in $\mathbf{A}/\theta$ is the same as the extended labelling of $\langle 0,1\rangle$ in $(\mathbf{A}+f)/\theta$. We know that the extended labelling of $\langle\theta,1\rangle$ in $\mathbf{A}$ is the same as the extended labelling of $\langle 0,1\rangle$ in $\mathbf{A}/\theta$, see [7, Lemma 2.18]. Hence, the extended labelling of $\langle 0,1\rangle$ in $(\mathbf{A}+f)/\theta$ is the same as the extended labelling of $\langle\theta,1\rangle$ in $\mathbf{A}+f$. Therefore, we obtain the statement. □

Lemma 3.15. *Let $\mathbf{A}$ be a finite uniform Mal'cev algebra with congruence lattice $\{0,\theta,1\}$. If $[1,1] \geq \theta$, $[1,\theta] = \theta$ and $[\theta,\theta] = 0$, then $\mathbf{A}$ is polynomially equivalent to an expanded group.*

Proof. Let $m, n \in \mathbb{N}$ be such that $|A/\theta| = m + 1$ and $|a/\theta| = n + 1$ for all $a \in A$. There is a suitable θ-enumeration a_{ij} of the elements of A by Lemma 3.7 because $[\theta, \theta] = 0$. We know that there exists a polynomial group operation $+$ on the set A/θ by Proposition 3.2 because $\mathbf{A}/\theta$ is simple. Now we take the $(\theta, +)$ corresponding first index binary operation $\oplus$ on $\{0, \dots, m\}$. We know that $\oplus$ is a group operation by Corollary 2.7. We define $+$ on $\{0, \dots, n\}$ as in (3.2).

Finally, the index defined operation $f_{\oplus,+}$ we denote shortly by f. Obviously, f is a congruence preserving group operation on A. We notice that $\mathbf{A}$ satisfies $(0 : \theta) \leq \theta$ and therefore, the (SC1)-property. Hence, $\mathbf{A}$ is weakly polynomially rich by [8, Theorem 24, Theorem 31]. Therefore, f is a polynomial if it preserves the extended labelling. First, we notice that f/θ is a polynomial of $\mathbf{A}/\theta$ using Proposition 3.4. Hence, f preserves the extended labelling of $\langle \theta, 1 \rangle$ by Lemma 3.14. In Lemma 3.13, we have proved that f preserves the extended labelling of $\langle 0, \theta \rangle$. □

Proposition 3.16. *Let* $\mathbf{A}$ *be a finite Mal'cev algebra such that* $[1, 1] = 1$. *If there exists a coatom* θ *in the congruence lattice of* $\mathbf{A}$ *such that* $[\theta, 1] = 0$, *then* $\mathbf{A}$ *is polynomially equivalent to an expanded group.*

Proof. Let T be a transversal of A through the classes modulo θ. Let $\cdot$ be any group operation on T with neutral element $o \in T$. To make the notation simpler, we introduce $x +_o y := d(x, o, y)$ and $x -_o y := d(x, y, o)$, for all $x, y \in A$. We extend $\cdot$ to A by

$$x_1 \cdot x_2 := ((x_1 -_o t_1) +_o (x_2 -_o t_2)) +_o t_1 \cdot t_2$$

for all $x_1,\ x_2 \in A$ and $t_1,\ t_2 \in T$ such that $x_1 \equiv_\theta t_1$ and $x_2 \equiv_\theta t_2$. Then $\cdot$ is a polynomial operation of $\mathbf{A}$ by [2, Theorem 3.3].

We have $(x +_o y) +_o z = x +_o (y +_o z)$ for all $x, y, z \in o/\theta$, using the fact $[\theta, \theta] = 0$ and [2, Proposition 2.6]. Therefore, one can show that $(x_1 \cdot x_2) \cdot x_3 = x_1 \cdot (x_2 \cdot x_3)$ for all $x_1, x_2, x_3 \in A$ by [2, Proposition 2.7(4)].

Let $a, b \in A$. We prove that there is a solution of the equation $xa = b$. Let $t_2, t \in T$ be such that $a \equiv_\theta t_2$ and $b \equiv_\theta t$. We know that there exists a unique $t_1 \in T$ such that $t_1 \cdot t_2 = t$. Now we have to find $x \equiv_\theta t_1$ such that $((x -_o t_1) +_o (a -_o t_2)) +_o t = b$. We prove that $x = ((b -_o t) -_o (a -_o t_2)) +_o t_1$ is a solution of the last equation. We substitute $((b -_o t) -_o (a -_o t_2)) +_o t_1$ for x and use [2, Proposition 2.7] several times to calculate

$$\begin{aligned}
&\Big(\Big(\big(((b -_o t) -_o (a -_o t_2)) +_o t_1\big) -_o t_1\Big) +_o (a -_o t_2)\Big) +_o t \\
&= \big(((b -_o t) -_o (a -_o t_2)) +_o (a -_o t_2)\big) +_o t && \text{since } (b -_o t) -_o (a -_o t_2) \equiv_\theta o \\
&= (b -_o t) +_o t && \text{since } (b -_o t) \equiv_\theta (a -_o t_2) \\
&= b && \text{since } b \equiv_\theta t.
\end{aligned}$$

Similarly, one can obtain that for all $a, b \in A$, the equation $ax = b$ has a solution. Hence, $\cdot$ is a group operation and $\mathbf{A}$ is polynomially equivalent to an expanded group. □

4. Expanded loops

Proposition 4.1. *Let* $\mathbf{A}$ *be a nilpotent Mal'cev algebra. Then* $\mathbf{A}$ *is polynomially equivalent to an expanded loop.*

Proof. We know that $D(x, y, z) := d(z, y, x)$, for all $x, y, z \in A$, is also a Mal'cev term of $\mathbf{A}$. Therefore, the functions $x \mapsto d(x, b, c)$ and $y \mapsto D(y, b, a)$ are bijective for all $b, c \in A$, by [6, Corollary 7.4]. Hence, $y \mapsto d(a, b, y)$ is bijective for all $a, b \in A$. Now the operation $(x, y) \mapsto d(x, o, y)$ is a quasigroup operation with the neutral element o. □

Theorem 4.2. *Let* $\mathbf{A}$ *be a finite uniform Mal'cev algebra with congruence lattice* $\{0, \theta, 1\}$. *Then* $\mathbf{A}$ *is polynomially equivalent to an expanded loop.*

Proof. We analyze the value of the commutator $[1, 1]$ on the congruence lattice of $\mathbf{A}$.

The case $[1, 1] = 0$: Then $\mathbf{A}$ is abelian. In this case, $\mathbf{A}$ is polynomially equivalent to a module over a ring. Hence, we obtain the statement.

The case $[1, 1] = 1$: There are two subcases.

$[1, \theta] = 0$: The statement follows from the Proposition 3.16.

$[1, \theta] = \theta$: If $[\theta, \theta] = 0$, then we use Lemma 3.15. If $[\theta, \theta] = \theta$, then θ is non-abelian. Proposition 3.5 yields the statement.

The case $[1, 1] = \theta$: There are two subcases.

$[1, \theta] = 0$: Then $[1, [1, 1]] = 0$, and therefore $\mathbf{A}$ is nilpotent. We obtain the statement by Proposition 4.1.

$[1, \theta] = \theta$: If $[\theta, \theta] = \theta$, then θ is non-abelian and we use Proposition 3.5. If $[\theta, \theta] = 0$, then we use Lemma 3.15. □

Theorem 4.3. *Let* $\mathbf{A}$ *be a finite uniform Mal'cev algebra with congruence lattice of height at most* 2. *Then* $\mathbf{A}$ *is polynomially equivalent to an expanded loop.*

Proof. First, let $\mathbf{A}$ be simple. Then $\mathbf{A}$ is polynomially equivalent to an expanded group, by Proposition 3.2. For nonsimple Mal'cev algebras, the congruence lattice of height two can be:

(1) the three element chain; then we obtain the statement by Theorem 4.2.

(2) isomorphic to $\mathbf{M}_2$; then we obtain the statement by Proposition 3.3.

(3) isomorphic to $\mathbf{M}_i$ for $i \geq 3$; then we obtain the statement by Proposition 3.1. □

Acknowledgements. The author thanks E. Aichinger and K. Kaarli for useful discussions during the work on this paper.

References

[1] Aichinger, E.: On Hagemann's and Herrmann's characterization of strictly affine complete algebras. Algebra Universalis **44**, 105–121 (2000)
[2] Aichinger, E.: The polynomial functions of certain algebras that are simple modulo their center. Contributions to General Algebra vol. 17, pp. 9–24 (2006)
[3] Aichinger, E., Mudrinski, N.: Some applications of higher commutators in Mal'cev algebras. Algebra Universalis **63**, 367–403 (2010)
[4] Chajda, I., Eigenthaler, G., Länger, H.: Congruence Classes in Universal Algebra. Heldermann, Lengo (2003)
[5] Freese, R.: Subdirectly Irreducible Algebras in Modular Varieties. In: Proceedings of the Conference on Universal Algebra and Lattice Theory (Puebla 1982). Lecture Notes in Mathematics vol. 1004, pp. 142–152. Springer, Berlin (1983)
[6] Freese, R., McKenzie, R.N.: Commutator Theory for Congruence Modular Varieties. Cambridge University Press, Cambridge (1987)
[7] Hobby, D., McKenzie, R.N.: The Structure of Finite Algebras. AMS Contemporary Mathematics, vol. 76. Providence (1988)
[8] Idziak, P.M., Słomczyńska, K.: Polynomially rich algebras. J. Pure Appl. Algebra **156**, 33–68 (2001)
[9] Kaarli, K.: Finite uniform lattices are congruence permutable. Acta Sci. Math. (Szeged) **71**, 457–460 (2005)
[10] Kaarli, K., Mayr, P.: Polynomial functions on subdirect products. Monatsh. Math. **159**, 341–359 (2010)
[11] McKenzie, R.N.: Narrowness implies uniformity. Algebra Universalis **15**, 67–85 (1982)
[12] McKenzie, R.N., McNulty, G.F., Taylor, W.F.: Algebra, Lattices, Varieties, vol. 1. Wadsworth Brooks/Cole Advanced Books Software, Monterey (1987)
[13] Taylor, W.: Uniformity of congruences. Algebra Universalis **4**, 342–360 (1974)

Nebojša Mudrinski

Institut für Algebra, Johannes Kepler Universität, 4040 Linz, Austria & Department of Mathematics and Informatics, Faculty of Sciences, University of Novi Sad, Trg Dositeja Obradovića 4, 21000 Novi Sad, Serbia
e-mail: nmudrinski@dmi.uns.ac.rs